UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,718	03/04/2002	Martin Hurich	10191/2275	4797

26646 7590 02/22/2006

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 02/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/090,718	HURICH, MARTIN	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed November 21, 2005, have been fully considered but they are not persuasive.

2. Claims 1-16 are pending and have been examined.

Response to Amendment

3. Applicant has not filed a certified copy of application **10110049.3,** filed in Germany, as required by 35 U.S.C. 119(b).

4. The objections to the specification are not withdrawn.

5. The rejections under 35 USC § 101 are not withdrawn.

6. Kawano et al. (US Patent 5,995,623, hereinafter Kawano) teach encrypting information to be transmitted so that no byte-wise allocation between input and output data occurs (hashing). Kawano selects pieces of information to be encrypted, thus provides the architecture to perform the claimed invention.

7. Furthermore, stream ciphers applied to a "complete stream" were conventional and well known, as it was to apply hash functions to the encrypted content (Menezes et al., chapter 9, hereinafter Menezes).

Priority

8. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Germany on March 2, 2001. It is noted, however, that applicant has not filed a certified copy of the **10110049.3** application as required by 35 U.S.C. 119(b).

Specification

9. The disclosure is objected to because of the following informalities: "ASIC" (page 4, line 9), "EEPROMs", "CD ROMs" (page 4, line 12). While well known in the art, these terms have not been defined.

10. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: "byte-wise allocation between input and output data occurs" (claims 1, 7, 11, 13, 15-16). It is not clear what a "byte-wise allocation between input and output data occurs" is, the specification does not define what "byte-wise allocation" is and examiner cannot determine what it is.

11. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: "a program code arrangement" (claims 15-16). It is not clear what a "program code arrangement" is, the specification does not limit the program code to a functional version of the code, but could include non-functional versions of the code.

Claim Rejections - 35 USC § 112

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "transmitting/decrypting the encrypted data". There is insufficient antecedent basis for these limitations in the claim.

Claim Rejections - 35 USC § 101

14. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

15. Claims 11-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 11 and 13 state "a computer program for execution"; a computer program is considered non-statutory subject matter according to the MPEP, 2106, paragraph IV.B:

> *"Since a computer program is merely a set of instructions capable of being executed by a computer, the computer program itself is not a process and Office personnel should treat a claim for a computer program, without the computer-readable medium needed to realize the computer program's functionality, as nonstatutory functional descriptive material. When a computer program is claimed in a process where the computer is executing the computer pro-gram's instructions, Office personnel should treat the claim as a process claim. See paragraph IV.B.2(b), below. When a computer program is recited in conjunction with a physical structure, such as a computer memory, Office personnel should treat the claim as a product claim. See paragraph IV.B.2(a), below".*

Additionally, Applicant has used the phrase **"program code arrangement for"** in what appears to be an effort to distinguish from **"program code for."** Since the specification fails to provide a description of Applicant's intent for the word "arrangement," it would have been reasonably interpreted by one of ordinary skill in the art to be intended to cover something broader than a functional version of the program code itself. Thus, it is believed to cover a non-functional descriptive material version of the code and additionally be non-statutory based on that rationale.

Dependent claims 12 and 14 fail to resolve the deficiencies of the claim from which they depend and are rejected based on their dependency from claim 11.

Claims 15-16 state "**computer readable medium, comprising a program code arrangement**". Since it is unclear what a "**program code arrangement**" is intended to cover, and a program code arrangement is believed to reasonably be interpreted as not being the code itself, but to include a non-executable and thus non-functional descriptive material version of the code for the reasons above, these claims are not believed to be limited to statutory embodiments.

16. To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 103

17. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

18. Claims 1-4 and 6-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawano, and further in view of Menezes.

Regarding claim 1, Kawano teaches encrypting data to be transmitted in a programming unit using a first key, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs (column 17, lines 1-67); transmitting the encrypted data to the control unit via a data line (column 17, lines 1-67); and decrypting

the encrypted data in the control unit using a second key provided in the control unit (column 16, lines 1-67, column 17, lines 1-67). Kawano does not expressly disclose encrypting a complete stream of data. However, Menezes teaches encrypting a complete stream of data (sections 9.1, 9.3, and 9.5-9.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the complete stream of data on the system of Kawano. One of ordinary skill in the art would have been motivated to perform such a modification to increase security and provide for message authentication (Menezes, section 9.1).

Regarding claim 7, Kawano teaches a programming unit in which a first key is provided (column 17, lines 1-67); a control unit in which a second key is provided (column 17, lines 1-67); and a data line coupled to the programming unit and the control unit for transmitting encrypted data, the encrypted data being an encryption of a stream of data, wherein no byte-wise allocation between input and output data occurs (column 16, lines 1-67, column 17, lines 1-67); Kawano does not expressly disclose encrypting a complete stream of data. However, Menezes teaches encrypting a complete stream of data (sections 9.1, 9.3, and 9.5-9.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the complete stream of data on the system of Kawano. One of ordinary skill in the art would have been motivated to perform such a modification to increase security and provide for message authentication (Menezes, section 9.1).

Regarding claim 11, Kawano teaches a program code arrangement for performing an encryption of a stream of data in accordance with a table and a hash

function, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs (column 15, lines 1-67, column 16, lines 1-67, column 17, lines 1-67). Kawano does not expressly disclose encrypting a complete stream of data. However, Menezes teaches encrypting a complete stream of data (sections 9.1, 9.3, and 9.5-9.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the complete stream of data on the system of Kawano. One of ordinary skill in the art would have been motivated to perform such a modification to increase security and provide for message authentication (Menezes, section 9.1).

Regarding claim 13, Kawano teaches a program code arrangement for performing a decryption of a stream of data in accordance with a table and a hash function wherein a byte by byte decryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs (column 15, lines 1-67, column 16, lines 1-67, column 17, lines 1-67). Kawano does not expressly disclose decrypting a complete stream of data. However, Menezes teaches decrypting a complete stream of data (sections 9.1, 9.3, and 9.5-9.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the complete stream of data on the system of Kawano. One of ordinary skill in the art would have been motivated to perform such a modification to increase security and provide for message authentication (Menezes, section 9.1).

Regarding claim 15, Kawano teaches a program code arrangement for performing an encryption of a stream of data in accordance with a table and a hash function, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs (column 15, lines 1-67, column 16, lines 1-67, column 17, lines 1-67). Kawano does not expressly disclose encrypting a complete stream of data. However, Menezes teaches encrypting a complete stream of data (sections 9.1, 9.3, and 9.5-9.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the complete stream of data on the system of Kawano. One of ordinary skill in the art would have been motivated to perform such a modification to increase security and provide for message authentication (Menezes, section 9.1).

Regarding claim 16, Kawano teaches a program code arrangement for performing a decryption of a stream of data in accordance with a table and a hash functions wherein a byte by byte decryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs (column 15, lines 1-67, column 16, lines 1-67, column 17, lines 1-67). Kawano does not expressly disclose decrypting a complete stream of data. However, Menezes teaches encrypting a complete stream of data (sections 9.1, 9.3, and 9.5-9.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the complete stream of data on the system of Kawano. One of ordinary skill in the art would have been motivated to perform such a

modification to increase security and provide for message authentication (Menezes, section 9.1).

Regarding claims 2 and 8, the combination of Kawano and Menezes teaches wherein the first key and the second key are identical (Kawano, columns 17, lines 10-67, column 18, lines 1-25).

Regarding claims 3 and 9, the combination of Kawano and Menezes teaches wherein the first key and the second key are not identical (Kawano, columns 17, lines 1-67, column 18, lines 1-67) and Menezes (sections 9.1, 9.3, and 9.5-9.6).

Regarding claim 4, the combination of Kawano and Menezes teaches wherein each one of the first key and the second key includes a table that is accessed by a hash function (Kawano, column 15, lines 1-67).

Regarding claim 6, the combination of Kawano and Menezes teaches wherein at least one of the first key and the second key is implemented in the form of a computer program (Kawano, column 9, lines 1-67, column 10, lines 1-67).

Regarding claim 10, the combination of Kawano and Menezes teaches wherein the programming unit and the control unit each includes an electronic computing unit and a memory module that are linked together by a data bus (Kawano, column 16, lines 1-67, column 17, lines 1-67, figure 12).

Regarding claim 12, the combination of Kawano and Menezes teaches wherein the computing unit includes an electronic computing unit in a programming unit (Kawano, column 16, lines 1-67, column 17, lines 1-67, figure 12).

Regarding claim 14, the combination of Kawano and Menezes teaches wherein the computing unit includes an electronic computing unit in a control unit (Kawano, column 16, lines 1-67, column 17, lines 1-67, figure 12).

19. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kawano and Menezes, and further in view of Nohda (US Patent Number: 6,215,875).

Regarding claim 5, the combination of Kawano and Menezes does not disclose expressly wherein at least one of the first key and the second key is implemented in an electronic circuit. However, Nohda teach implementing a key in an electronic circuit (column 7, lines 5-30). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement at least one key using an electronic circuit. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made it was well known in the art to implement ciphering algorithms using hardware (Nohda, column 2, lines 10-50).

Conclusion

20. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

21. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

24. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DGC